



# Dacorum Borough Council

## Final Internal Audit Report

### Customer Relationship Management (CRM) System

September 2017

This report has been prepared on the basis of the limitations set out on page 9.

CONFIDENTIAL

**Distribution List:**

Mark Housden – Contract Manager  
Ben Hosier – Group Manager (Commissioning, Procurement and Compliance)  
David Skinner – Assistant Director (Finance & Resources)  
James Deane – Corporate Director (Finance & Operations) (Final Report Only)  
Sally Marshall – Chief Executive (Final Report only)

**Key Dates:**

Date of draft report: October 2016/April 2017  
Receipt of responses: March 2017/August 2017  
Date of final report: September 2017

This report and the work connected therewith are subject to the Terms and Conditions of the Contract dated 1 April 2015 between Dacorum Borough Council and Mazars Public Sector Internal Audit Limited. This report is confidential and has been prepared for the sole use of Dacorum Borough Council. This report must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law, we accept no responsibility or liability to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.

## Contents

1. Executive Summary .....	1
2. Scope of Assignment .....	3
3. Assessment of Control Environment.....	4
4. Observations and Recommendations .....	5
<b>Recommendation 1: Generic CRM Accounts (Priority 2) .....</b>	<b>5</b>
<b>Recommendation 2: Microsoft Dynamics CRM 2013 Upgrade Path (Priority 3) .....</b>	<b>6</b>
Appendix A - Reporting Definitions .....	7
Appendix B - Staff Interviewed.....	8
Statement of Responsibility.....	9

# 1. Executive Summary

## 1.1. Background

In 2013, the Council went out to tender for the Customer Service Centre Gateway programme, which was won by Northgate. There are two distinct streams to this programme:

- The Channel Shift Project, which is still evolving and changing; and
- The Customer Relationship Management (CRM) System is used by the Customer Service Team that was previously part of the Council and is now part of Northgate.

## 1.2. Audit Objective and Scope

The overall objective of this audit was to provide an independent assurance over the design and operation of the control environment established and applied to the Customer Relationship Management (CRM) System, which Northgate currently manage and support on behalf of the Council and provide any potential recommendation guidance on how to improve the current controls framework going forward.

In summary, the audit scope covered the following areas:

- Application Management and Governance
- System Access Security
- Interfaces and Data Flow
- Data Input and Output Controls
- Change Control and
- Support Arrangements

Further detail on the scope of the audit is provided in Section 2 of the report.

## 1.3. Summary Assessment

Our audit of Dacorum Borough Council's internal controls operating in respect of the Customer Relationship Management (CRM) System found that there is a sound system of internal control designed to achieve the system objectives. Also, there is testing evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below:

Evaluation Assessment	Testing Assessment
Full	Substantial

Management should be aware that our internal audit work was performed according to UK Public Sector Internal Audit Standards (PSIAS) which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Similarly, the assessment gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the Customer Relationship Management (CRM) System control environment is shown in Section 3.

#### 1.4. **Key Findings**

One priority 2 recommendation and one priority 3 recommendation were raised where we believe there is scope for improvement within the CRM application control environment. These are set out below:

- Assignment of the Administration Account rights to specific users. (Priority 2)
- Upgrade of the plan from CRM 2013 to CRM 2016 (Priority 3)

Full details of the audit findings and recommendations are shown in Section 4 of the report.

#### 1.5. **Management Response**

The management responses have been included in the main body of the report.

#### 1.6. **Acknowledgement**

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

## 2. Scope of Assignment

### 2.1. Objective

The overall objective of this compliance audit was to provide assurance on the design and operation of the controls applied in respect of the Customer Relationship Management (CRM) System.

### 2.2. Approach and Methodology

The audit approach was developed by an assessment of risks and management controls operating within each area of the scope and the following procedures were adopted to enable us to recommend control improvements:

- Hold discussions with key members of staff to ascertain the operational controls;
- Identification of the role and objective of each area of scope;
- Identification of risks relating to the auditable area and the controls in place that enable the control objectives to be achieved;
- Evaluation and testing of controls within the system;
- Discussion of our findings with management and further development of our recommendations; and
- Preparation and agreement of a draft report with the process owner.

### 2.3. Areas Covered

The audit was carried out to evaluate and test controls over the following areas:

- **Application Management and Governance:** - Adequate system governance arrangements are in place relating to the ownership and administration of the system as well as consideration for the management of licenses. Furthermore, controls are in place to support the appropriate processing of data in accordance with its sensitivity.
- **System Access Security:** - Logical access procedures are in place to restrict access to the application to only authorised individuals and these procedures are supported by effective password controls and audit trails. Furthermore, permissions are assigned to authorised users when required and enforce separation of duties.
- **Interface Controls and Data Flow:** - Data flows and system processing requirements have been identified and mapped. Furthermore, processes are in place to reconcile data that is transferred both from and to the application to help ensure that these transfers are complete and accurate.
- **Data Input and Output:** - Data input controls are in place to help ensure the accuracy and completeness of data that is entered onto the system through appropriate authorisation and on-screen validation. Adequate controls are in place to help ensure that data output meets the needs of the service and is reconciled to confirm its accuracy. Furthermore, exception and rejection reports are available to assist the management and identification of potentially inaccurate data.
- **Change Control:** - Changes to the application are applied in a controlled manner and are subject to authorisation. Adequate documentation is created and retained to support the changes that have been implemented.
- **Support Arrangements:** - Procedures are in place to help ensure that the application is supported as per the contractual arrangements and that access by third parties is appropriately controlled.

### 3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

Control Objectives Assessed	Design of Controls	Operation of Controls	Recommendations Raised
Application Management and Governance			
System Security			<b>Recommendation 1</b>
Interface Controls and Data Flow			
Data Input and Output			
Change Control			<b>Recommendation 2</b>
Support Arrangements			

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

## 4. Observations and Recommendations

### Recommendation 1: Generic CRM Accounts (Priority 2)

<p><b>Recommendation</b></p> <p>All of the Microsoft Dynamics Customer Relationship Management 2013 application system accounts with input rights, should be assigned to specifically named users.</p>
<p><b>Observation</b></p> <p>Section 5 of the Corporate IT Security Policy necessitates that “The Each user must have a unique User ID and a password” that should not be shared between users to help ensure that users are accountable for their actions.</p> <p>Examination of the Microsoft Dynamics Customer Relationship Management 2013 application system user list, identified that four of the 32 CRM accounts have been assigned generic account names. (This includes the system administration account).</p> <p>Unless all system accounts and access rights are assigned to specifically named users, there is a risk that system accountability will be compromised.</p>
<p><b>Responsibility</b></p> <p><b>Rob Smyth, Assistant Director – Performance, People and Innovation</b></p>
<p><b>Management response / deadline</b></p> <p>DBC ICT’s own policy is to not allow input rights for generic accounts with no specified user. However in this case (and in line with the agreed contract and approach between DBC and Northgate PS) DBC makes use of an instance of Microsoft Dynamics that is hosted within Northgate’s data centre and within their network domain.</p> <p>CRM and associated user accounts are therefore administered exclusively by Northgate and as a result, DBC ICT does not have sight of or control over accounts created within Northgate’s domain. However, DBC ICT were involved in the commissioning of this contract including the evaluation, award and implementation processes.</p> <p>Nevertheless it is worth noting there are circumstances where the use of service accounts (rather than named users) can be appropriate. For example, apparently generic accounts with appropriately limited permissions (such as the disabling of interactive login) might be used for specific purposes within an automated process.</p> <p>It is also important to note that access to the system is enabled by a one-way trust relationship between domains – that is to say that Northgate’s domain trusts Dacorum’s domain but not vice versa. This greatly limits the Council’s exposure to vulnerabilities within Northgate’s network and applications.</p> <p>Going forward, DBC is bringing control of CRM back in-house and as a result, we will be in a position to ensure that management of the system, accounts and permissions will be in line with DBC ICT policy. Expected to have all in place by end of January 2018.</p>

**Recommendation 2: Microsoft Dynamics CRM 2013 Upgrade Path (Priority 3)**

<p><b>Recommendation</b></p> <p>Formal consideration should be given to the financial and resource requirements for the upgrade transition path and timeframe from the current CRM 2013 application version to the CRM 2016 version.</p>
<p><b>Observation</b></p> <p>Upgrading to the current application system version helps to ensure that application systems can be adequately supported by the vendor.</p> <p>Examination of the system configuration settings identified that the Microsoft Dynamics CRM 2013 application is currently in use and licenced to DBC. Subsequent examination of the vendor website identified that Microsoft Dynamics CRM 2016 is the latest version of the CRM application and that mainstream support for the CRM 2013 version ends in January 2019.</p> <p>There is a potential risk that the application system may not be adequately supported by the vendor unless effective planning arrangements are established to transition from the current CRM 2013 version to the CRM 2016 version.</p>
<p><b>Responsibility</b></p> <p>Ben Trueman – Group Manager for Technology &amp; Digital Transformation</p>
<p><b>Management response / deadline</b></p> <p>DBC recognises the importance of keeping applications up-to-date.</p> <p>However, the existing contract stated that Northgate PS would provide CRM 2013 as its platform and as is this is their product (hosted in their data centre), any decision about upgrading will be made in line with their own roadmap and timetable.</p> <p>DBC have been in conversation with Northgate PS for several months to gain assurance that the current instance would be upgraded. However, during the course of these discussions, Northgate announced that they would be withdrawing their CRM product from the market.</p> <p>As a result they will not be undertaking any upgrades, although they have said they will honour the existing support agreements.</p> <p>It is important to note that DBC is putting in place plans to replace the existing Northgate PS hosted CRM solution with our own (and new) instance of our own MS Dynamics CRM 2016.</p> <p>This will enable us to ensure that the product is regularly upgraded, fully supported by the vendor and that we can take advantage of new functionality as well as broader changes in our application estate. Expected to have all in place by end of January 2018.</p>

## Appendix A - Reporting Definitions

### Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
<b>Full</b>		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
<b>Substantial</b>		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
<b>Limited</b>		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
<b>Nil</b>		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

### Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
<b>Priority 1</b>	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
<b>Priority 2</b>	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
<b>Priority 3</b>	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
<b>System Improvement Opportunity</b>	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

## Appendix B - Staff Interviewed

The following personnel were consulted:

Audit sponsor: David Skinner – Assistant Director (Finance & Resources)

Audit Contacts: Mark Housden – Contract Manager

Ben Hosier – Group Manager (Commissioning, Procurement and Compliance)

Ben Trueman – Group Manager (Technology & Digital Transformation)

Rob Smyth – Assistant Director (Performance, People and Innovation)

Auditee Contacts: Ingrid Johnson – Client Services Director – Northgate Public Services

Tracy Lancashire – Strategic Operations Manager – Northgate Public Services

Lee Lewis – Customer Service Advisor – Northgate Public Services

We would like to thank the staff involved for their co-operation during the audit.

## Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

### **Mazars Public Sector Internal Audit Limited**

**London**

**September 2017**

This document is confidential and prepared solely for your information. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.